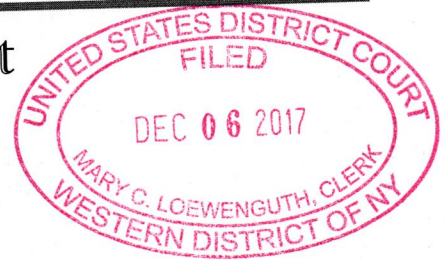


**United States District Court**  
for the  
Western District of New York



**In the Matter of the Search of**

*(Briefly describe the property to be searched or identify the person by name and address.)*

See Description of Items to be Searched, attached hereto as Attachment A

**Case No. 17-MJ- 155**

**APPLICATION FOR SEARCH WARRANTS**

I, a federal law enforcement officer or an attorney for the government, request search warrants and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Description of Items to be Searched, attached hereto as Attachment A,

located in the Western District of New York, there is now concealed *(identify the person or describe the property to be seized)*:

The items set forth on Attachment B, Items to be Seized.

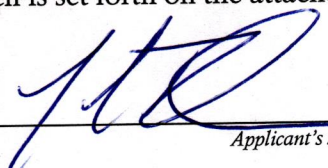
The basis for search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of Title 18, United States Code, Sections 2251, 2252, and 2252A.

The application is based on these facts:

- ☒ continued on the attached sheet.
- ☐ Delayed notice of \_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.


  
\_\_\_\_\_  
*Applicant's signature*

JUSTIN BURNHAM  
SPECIAL AGENT  
HOMELAND SECURITY INVESTIGATIONS  
\_\_\_\_\_  
*Printed name and title*

Sworn to before me and signed in my presence.

Date: December 6, 2017

City and state: Buffalo, New York

  
\_\_\_\_\_  
*Judge's signature*

H. KENNETH SCHROEDER, JR.  
UNITED STATES MAGISTRATE JUDGE  
\_\_\_\_\_  
*Printed name and Title*

**AFFIDAVIT IN SUPPORT OF SEARCH WARRANT**

STATE OF NEW YORK     )  
COUNTY OF ERIE        )     SS:  
CITY OF BUFFALO        )

I, Justin J. Burnham, being duly sworn, depose and say:

1. I am a Special Agent with Homeland Security Investigations (HSI) and have been so employed since October 2008. I am currently assigned to the Buffalo Field Office of HSI and am assigned to the Child Exploitation Unit (CEU). As a member of the CEU, I investigate the sexual exploitation of children, including possession, receipt and the production of child pornography as well as coercion and enticement, in violation of Title 18, United States Code, Sections 2252, 2252A, and 2422. I have received specialized training in the area of child pornography, child exploitation, and coercion and enticement, and I have had the opportunity to observe and review numerous examples of child pornography, as defined in Title 18 United States Code, Section 2256(8).

2. This affidavit is submitted in support of an application for a search warrant for electronic devices described in Attachment A of this Affidavit, herein the "SUBJECT DEVICES", for contraband and evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2251, 2252, and 2252A, which items are more specifically described in Attachment B of this Affidavit.



3. The statements in this affidavit are based in part on information provided by Canadian law enforcement officials; the New York State Police; the Chautauqua County Sheriff's Office, and on my investigation of this matter. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2251 (Sexual exploitation of children); 18 U.S.C. § 2252 (Certain activities relating to material constituting or containing images of minors engaging in sexually explicit conduct); or 18 U.S.C. § 2252A (Certain activities relating to material constituting or containing child pornography) are presently located in the SUBJECT DEVICES.

4. As noted above, this investigation concerns alleged violations of the following:
- a. Title 18, United States Code, Sections 2251(d) and (e) prohibit any person from knowingly making, printing, or publishing, or causing to be made, printed, or published, or attempting or conspiring to make, print, publish, or attempt or conspire to cause to be made, printed, or published, any notice or advertisement seeking or offering to receive, exchange, buy, produce, display, distribute, or reproduce, any visual depiction, if the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct; or participation in any act of sexually explicit conduct by or with any minor for the purpose of producing a visual depiction of such conduct.
  - b. Title 18, United States Code, Sections 2252(a)(1) and (b)(1) prohibit any person from knowingly transporting or shipping, or attempting or conspiring to transport or ship, any visual depiction using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce, by any means including by computer or mails, if the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

- c. Title 18, United States Code, Sections 2252A(a)(5)(B) and (b)(2) prohibit a person from knowingly possessing or knowingly accessing with intent to view, or attempting or conspiring to do so, any material that contains an image of child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

#### **SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS**

5. Based upon my training and experience and information related to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact disks, magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained by corporations, including but not limited to "cloud" storage. I also know that during the search of the premises it is not always possible to search computer equipment and storage devices for data for a number of reasons, including the following:

- a. Searching computer systems is a highly technical process which requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software application, or operating system that is being searched;



b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover “hidden,” erased, compressed, encrypted, or password-protected data. Computer hardware and storage devices may contain “booby traps” that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted;

c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises; and

d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension “.jpg” often are image files; however, a user can easily change the extension to “.txt” to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a “dongle” or “keycard,” is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called “steganography.” For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial

amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is contraband, evidence, fruits, or instrumentalities of a crime.

6. Based on my own experience and my consultation with other agents who have been involved in computer searches, searching computerized information for contraband, evidence, fruits, or instrumentalities of a crime often requires the seizure of all of a computer system's input and output peripheral devices, related software, documentation, and data security devices (including passwords), so that a qualified computer expert can accurately retrieve the system's data in a laboratory or other controlled environment. There are several reasons that compel this conclusion:

a. The peripheral devices that allow users to enter or retrieve data from the storage devices vary widely in their compatibility with other hardware and software. Many system storage devices require particular input/output devices in order to read the data on the system. It is important that the analyst be able to properly re-configure the system as it now operates in order to accurately retrieve the evidence listed above. In addition, the analyst needs the relevant system software (operating systems, interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media), as well as all related instruction manuals or other documentation and data security devices; and

b. In order to fully retrieve data from a computer system, the analyst also needs all magnetic storage devices, as well as the central processing unit (CPU).



Further, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software that may have been used to create the data (whether stored on hard drives or on external media) for proper data retrieval.

### **CRIMINAL COMPLAINT**

7. On October 16, 2017, Joseph HARVEY (hereinafter "HARVEY") was charged in the Western District of New York, by way of criminal complaint, for violating Title 18, United States Code, Sections 2252A(a)(2)(A) and 2252A(a)(5)(B). These charges were based on a joint investigation by the Toronto Police Service Child Exploitation Section and Homeland Security Investigations into HARVEY and his romantic partner Richard MILLER (hereinafter "MILLER"). This joint investigation revealed that between May 2015 and February 2016, MILLER and/or HARVEY used a web-based application to stream child pornography on the internet. This investigation also revealed that MILLER and/or HARVEY uploaded an image of child pornography to a Synchronoss Technologies, Inc. server on December 31, 2015. On May 13, 2017, a search was conducted, pursuant to a Federal Search Warrant, of 10464 Center Road, Forestville, New York, a home leased by HARVEY and MILLER. A search of a computer found in the home, conducted pursuant to the search warrant, revealed MILLER produced one video of child pornography involving himself and minor victim 1 as well as two pictures of suspected production of child pornography involving the person believed to be minor victim 1. The search also revealed that MILLER and/or HARVEY possessed approximately 202 videos of suspected child pornography, approximately 283 pictures of suspected child pornography and multiple

pictures and videos of bestiality.<sup>1</sup> Upon being questioned by HSI Agents, HARVEY admitted to viewing, via the internet, people of a "questionable age" have sexual intercourse.

8. On May 23, 2017, a Federal criminal complaint was filed against MILLER. At the initial appearance on the criminal complaint, an Order of Detention against defendant MILLER was signed by United States Magistrate Judge H. Kenneth Schroeder, Jr. and was filed on June 6, 2017.

9. On October 16, 2017, a Federal criminal complaint was filed against HARVEY, charging him with distribution, receipt, and possession of child pornography in violation of Title 18, United States Code, Sections 2252A(a)(2)(A) and 2252A(a)(5)(B). An Order of Detention against HARVEY was signed by Magistrate Judge Roemer and was filed on October 18, 2017.

10. In October 2017, Julia Harvey, sister of HARVEY, contacted HSI and said she had a telephonic conversation with HARVEY while he was detained pursuant to the aforementioned criminal charges. Julia Harvey said HARVEY asked her to go to his residence and retrieve a number of electronic items and personal mementos for safekeeping. According to Julia Harvey, she, along with Michelle Harvey and Carolyn Azzarella, who are also relatives of HARVEY, subsequently went to his residence and retrieved several electronic

---

<sup>1</sup> Notably, MILLER is facing state charges in New York State relating to abuse of animal by way of performing sexual acts with the animal.



devices (SUBJECT DEVICES) as well as some of HARVEY's personal belongings. After removing the SUBJECT DEVICES, they became concerned that they contained child pornography.

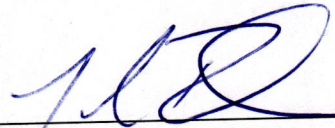
11. In October 2017, the United States Attorney's Office (USAO) received a telephone call from Michelle Harvey regarding the SUBJECT DEVICES. Michelle Harvey advised that HARVEY's family wanted to turn over the SUBJECT DEVICES to law enforcement as they were concerned about being in possession of child pornography.

12. On October 27, 2017, HSI Special Agent Justin Burnham interviewed Julia Harvey, Carolyn Azzarella, and Michelle Harvey regarding the SUBJECT DEVICES. During the course of the interviews, HSI SA Justin Burnham took possession of the SUBJECT DEVICES, which are more particularly described in Attachment A, from Julia and Michelle Harvey and secured them in the HSI computer forensic laboratory located in Buffalo, New York.

### CONCLUSION

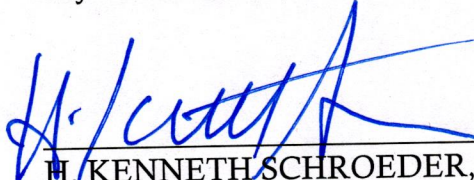
13. Based on the foregoing, there is probable cause to believe that the federal criminal statutes cited herein have been violated, and that the contraband, property, evidence, fruits and instrumentalities of these offenses, more fully described in Attachment B, are located in the SUBJECT DEVICES described in Attachment A. I respectfully request that this Court issue a search warrant for the SUBJECT DEVICES described in Attachment A, authorizing the seizure and search of the items described in Attachment B.

14. I am aware that the recovery of data by a computer forensic analyst takes significant time; much the way recovery of narcotics must later be forensically evaluated in a lab, digital evidence will also undergo a similar process. For this reason, the "return" inventory will contain a list of only the tangible items recovered from the premises. Unless otherwise ordered by the Court, the return will not include evidence later examined by a forensic analyst.

  
\_\_\_\_\_  
JUSTIN BURNHAM  
Special Agent  
Homeland Security Investigations

Sworn to before me this 6<sup>th</sup>

day of December , 2017.

  
\_\_\_\_\_  
H. KENNETH SCHROEDER, JR.  
United States Magistrate Judge



**ATTACHMENT A**

- A. Black Canon EOS Rebel T6 digital camera with lens bearing identification number 4476074772
- B. Black Tablet PC with white backing found in a white Tablet PC box with no observable serial number
- C. Black Amazon Kindle with no observable serial number
- D. Kodak Easy Share Z612 camera with a visibly worn serial number believed to be KCTFY64021656
- E. 10 - black, green, yellow and blue Imation, Memorex, and Fujifilm diskettes
- F. Motorola cellular telephone with gold/white cell phone case bearing model number XT1609 and IMEI number 354142074574502
- G. Black Verizon cellular telephone bearing serial number 511CQWC1339889
- H. Motorola cellular telephone with turquoise case bearing model number XT1609 and IMEI number 354142074574338
- I. Three CDs/DVDs
- J. Sandisk 32 GB memory card bearing reference number BM1628850844G
- K. Sandisk 4 GB thumb drive bearing reference numbers BH0901NRCB and SDCZ6-4096RB
- L. Hewlett Packard laptop computer bearing serial number CND6367D7B
- M. Three JVC mini DV cassette tapes
- N. One Sony mini DV cassette tape
- O. One 256 MB Kodak SD card bearing reference number 3401-256-CSKA

**ATTACHMENT B**

**ITEMS TO BE SEIZED**

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of Title 18, United States Code, Sections 2251, 2252 and 2252A:

1. Computers or storage media used as a means to commit the violations described above.
2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):
  - a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
  - b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
  - c. evidence of the lack of such malicious software;



- d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to the crime(s) under investigation and to the computer user;
- e. evidence indicating the computer user's knowledge and/or intent as it relates to the crimes under investigation;
- f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- g. evidence of programs (and associated data) that are designed to eliminate data from the COMPUTER;
- h. evidence of the times the COMPUTER was used;
- i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- k. records of or information about Internet Protocol addresses used by the COMPUTER;
- l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and
- m. contextual information necessary to understand the evidence described in this attachment.

3. Child pornography as defined in Title 18, United States Code, Section 2256(8), and child erotica.
4. Records, information, and items relating to violations of the statutes described above including:
  - a. Records, information, and items relating to the ownership of the SUBJECT DEVICES;
  - b. Records, information, and items relating to the ownership or use of computer equipment;
  - c. Records and information relating to the identity or location of the persons suspected of violating the statutes described above;
  - d. Records and information relating to the sexual exploitation of children, including correspondence and communications between users of "Application A";
  - e. Records and information showing access to and/or use of "Application A".

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic,



or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact discs, magnetic tapes, memory cards, memory chips, and other magnetic or optical media.